REMARKS

Entry of the foregoing amendment is respectfully requested. This amendment is intended to place the claims in a more conventional format and eliminate the multiple dependency of the claims.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: _____

James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: May 18, 2001

Attachment to Preliminary Amendment dated May 18, 2001

Marked-up Claims 1-12

1. (Amended) A method of controlling the use of a smart card comprising a microprocessor [able to effect] that executes cryptography calculations in the card for effecting authentication sessions at the time of a transaction between the card and a terminal, [characterised in that the said method uses] and at least one control counter, [(C_{KDP}) and in that, for a transaction comprising at least one authentication session by the card, the method consists] comprising the steps of:

- decrementing or incrementing the control counter by one unit [(u)] at the start of [the transaction] a transaction comprising at least one authentication session by the card, and

- if the authentication by the card has succeeded, [effecting the reincrementation or decrementation of the] subsequently incrementing or decrementing, respectively, said control counter by [the] said unit [(u)].

2. (Amended) A method according to Claim 1 [2, characterised in that] wherein the control counter [can count] counts down from or [count] counts up to a blocking value.

3. (Amended) A method according to Claim 2, [characterised in that it comprises the use of a] further including the step of using said control counter by [an] at least one encrypting key [and/or by a pair of encrypting keys] contained in the card.

Attachment to Preliminary Amendment dated May 18, 2001

Marked-up Claims 1-12

4. (Amended) A method according to Claim 3, [characterised in that] wherein the blocking value associated with a counter is a function of the type of transaction in which [the] an associated key [or the associated pair of keys] is used.

5. (Amended) A method according to Claim 3, [characterised in that] wherein the decrementation or incrementation unit of a control counter represents the number of cryptographic calculations with [the] an associated key [or the associated pair of keys,] performed up till then and including the one consisting of [the] said authentication session during [the] said transaction.

6. (Amended) A method according to Claim 3, [characterised in that] wherein the control counter associated with a key [or a pair of keys] is decremented or incremented by a new unit before each of the cryptographic calculations using [the] said key [or the said pair of keys] up to and including the one relating to [the] said authentication session by the card.

7. (Amended) A method according to Claim 5, [characterised in that the reincrementation or decrementation] wherein the subsequent incrementing or decrementing of the counter by the unit representing the number of cryptographic calculations is effected if the authentication session by the card has succeeded.

Attachment to Preliminary Amendment dated May 18, 2001

Marked-up Claims 1-12

8. (Amended) A method according to Claim 6, [characterised in that it comprises a pointing counter (D_{KDP}) for] further including the step of storing the number of decrementations or incrementations by one unit that have been carried out in a pointing counter, to [permit] control the [reincrementation or decrementation] subsequent incrementing or decrementing of the control counter [(C_{KDP})] via the content of the pointing counter, if the authentication session by the card has succeeded.

9. (Amended) A [control] method according to [any one of the preceding claims, characterised in that the] claim 1, wherein said authentication session by the card is effected at the time of a connection by direct link to a server.

10. (Amended) A method according to [any one of the preceding claims, characterised in that] claim 3 wherein, when the control counter is decremented, or incremented, up to a limit value, it blocks the use of the associated key [or associated pair of keys].

11. (Amended) A method according to Claim 10, [characterised in that] wherein the blocking of the use of the key [or pair of keys] is irreversible.

Attachment t Preliminary Amendment dated May 18, 2001

Marked-up Claims 1-12

12. (Amended) A smart card comprising at least one control counter associated with at least one key [and/or one pair of keys for implementing a control method according to any one of the preceding claims] and a microprocessor which executes the functions of decrementing or incrementing the control counter by one unit at the start of a transaction comprising at least one authentication session by the card, and subsequently incrementing or decrementing, respectively, said control counter by said unit if the authentication by the card has succeeded.